8

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/782,501	02/13/2001	Fred C. Thomas III	IOM-8034/P0717	9931

23377 7590 08/31/2004

WOODCOCK WASHBURN LLP
ONE LIBERTY PLACE, 46TH FLOOR
1650 MARKET STREET
PHILADELPHIA, PA 19103

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2131	6

DATE MAILED: 08/31/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/782,501	**Applicant(s)** THOMAS ET AL.	
	Examiner Longbit Chai	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *4*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

2. The effective filing date for the subject matter defined in the pending claims in this application is 02/13/2001.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 4, 12, 15, 18, 19, 21, 23, 25, 28 and 31 – 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Tycksen (Patent Number: US 6189097 B1), hereinafter referred to as Tycksen.

4. As per claims 1 and 19, Tycksen teaches a software authentication system for authenticating a communication channel between a plurality of software elements, comprising:

a. a host computer having host storage including a first software element (Tycksen: see for example, Column 1 Line 10 – 25);

b. a second software element to authenticate said first software element (Tycksen: see for example, Column 10 Line 10 – 26: Tycksen teaches the entire software authentication system can be decomposed into the following three different elements: (1) the first software element is the software object to be authenticated including the content integrity (2) the second software element is the certifying authority (Tycksen: see for example, Column 10 Line 11) – i.e., the software element to authenticate the desired software object by using asymmetric cryptographic keys, and (3) the proxy software, instantiated by the certifying authority, is the verifying process to conduct the validation process with the first software element (Tycksen: see for example, Column 10 Line 10));

c. wherein in response to said second software element making a request to said first software element for authentication of the first software element, the second software element retrieves a first encrypted digital signature from said host computer, the second software element retrieves a public key for use with said first encrypted digital signature and the second software element accesses at least one portion of a component stored in said host storage, said at least one portion of the accessed component is hashed to form a second digital signature (Tycksen: see for example, Column 10 Line 10 – 26);

d. wherein in response to receiving said encrypted first digital signature, said second software element decrypts said encrypted first digital signature with said public key and said second software element compares the first digital signature to the second digital signature; and whereupon the occurrence of a correlation between said first and second digital signatures, the first software element is authenticated (Tycksen: see for example, Column 10 Line 10 – 26).

5. As per claims 4 and 21, Tycksen teaches the claimed invention as described above (see claim 1 and 19 respectively). Tycksen further teaches the second software element instantiates a third software element which accesses said at least one portion of a component stored in said host storage in place of said accessing by said second software component (Tycksen: see for example, Column 10 Line 10 – 26: Tycksen teaches the entire software authentication system can be decomposed into the following three different elements: (1) the first software element is the software object to be authenticated including the content integrity (2) the second software element is the certifying authority (Tycksen: see for example, Column 10 Line 11) – i.e., the software element to authenticate the desired software object by using asymmetric cryptographic keys, and (3) the proxy software, instantiated by the certifying authority, is the verifying process to conduct the validation process with the first software element (Tycksen: see for example, Column 10 Line 10));

6. As per claim 12, Tycksen teaches the claimed invention as described above (see claim 1). Tycksen further teaches the first software element is a content providing software application (Tycksen: see for example, Column 7 Line 8 – 10 and Column 10 Line 34 – 35).

7. As per claims 15, and 28, Tycksen teaches the claimed invention as described above (see claim 1 and 19 respectively). Tycksen further teaches comprising a storage medium and a data storage device, wherein a communications channel between the data storage device and the storage medium is authenticated with a technique including at least one of a

retroreflective marker, latent illuminance marker, disk indelible utility mark (DIUM), holographic marker included on said storage medium (Tycksen: see for example, Column 1 Line 48).

8. As per claims 18 and 31, Tycksen teaches the claimed invention as described above (see claims 1 and 19 respectively). Tycksen further teaches said correlation occurs when one from the following group occurs: (1) when said first and second digital signatures are identical, (2) when a portion of said first digital signature is identical to a portion of second digital signature, (3) when said first digital signature equals said second digital signature after applying a predetermined algorithm to one of said first and second digital signatures and (4) when said first digital signature maps to said second according to an interpreted off-set match (Tycksen: see for example, Column 10 Line 11 – 26).

9. As per claim 23, Tycksen teaches the claimed invention as described above (see claim 19). Tycksen further teaches the accessing and hashing of said at least one portion of the component stored in host storage includes accessing and hashing at least one portion of the first software element (Tycksen: see for example, Column 10 Line 11 – 26).

10. As per claim 25, Tycksen teaches the claimed invention as described above (see claim 19). Tycksen further teaches the accessing and hashing of said at least one portion of the component stored in host storage includes the accessing and hashing of a file stored on a hard drive of said host (Tycksen: see for example, Column 6 Line 13 – 16).

11. As per claim 32, Tycksen teaches the claimed invention as described above (see claim 19). Tycksen further teaches a computer-readable medium having computer-executable instructions for instructing a computer to perform the method recited in claim 19 (Tycksen: see for example, Column 1 Line 1 – 19).

12. As per claim 33, Tycksen teaches the claimed invention as described above (see claim 19). Tycksen further teaches a modulated data signal carrying computer-executable instructions for performing the method as recited in claim 19 (Tycksen: see for example, Column 1 Line 1 – 19).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 2, 3, 5 – 8, 10, 16, 17, 20, 22, 24, 30, 34 – 37, 39 and 40 – 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tycksen (Patent Number: US 6189097 B1), hereinafter referred to as Tycksen, in view of Drake (Patent Number: 6006328), hereinafter referred to as Drake.

14. As per claim 34, Tycksen teaches a method of authentication of a software element, comprising:

a. said application instantiating a proxy driver software element (Tycksen: see for example, Column 10 Line 10 – 26: Tycksen teaches the entire software authentication system can be decomposed into the following three different elements: (1) the first software element is the software object to be authenticated including the content integrity (2) the second software element is the certifying authority (Tycksen: see for example, Column 10 Line 11) – i.e., the software element to authenticate the desired software object by using asymmetric cryptographic keys, and (3) the proxy software, instantiated by the certifying authority, is the verifying process to conduct the validation process with the first software element (Tycksen: see for example, Column 10 Line 10));

b. said proxy driver software element requesting authentication information from said device driver software element (Tycksen: see for example, Column 10 Line 10 – 26);

c. in response to said requesting of authentication information, transmitting a first encrypted digital signature from said host computer to said application, retrieving by said application a public key for use with said first encrypted digital signature, accessing by said proxy driver software element at least one portion of a component stored in the host storage, hashing said at least one portion to form a second digital signature (Tycksen: see for example, Column 10 Line 10 – 26);

d. in response to receiving said transmitted encrypted first digital signature, decrypting said encrypted first digital signature by said application with the public key and comparing the decrypted first digital signature to the second digital signature that is accessible to the application via said proxy driver software element (Tycksen: see for example, Column 10 Line 10 – 26); and

e. determining that said device driver software element is authenticated if said first digital signature correlates with said second digital signature (Tycksen: see for example, Column 10 Line 10 – 26).

15. Tycksen does not teach expressly the method is for authentication of a device driver software element stored in the memory of a host computer by an application.

16. Drake teaches the method is for authentication of a device driver software element stored in the memory of a host computer by an application (Drake: see for example, Column 16 Line 54 and Column 6 Line 13 – 16).

17. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Drake within the system of Tycksen because (a) Tycksen teaches the method of software authentication including content integrity (b) Drake discloses the software entity to be authenticated with pre-calculated check-data (and checksum) can be a keyboard device driver software prior to accepting the security ID-data (Drake: see for example, Column 6 Line 14, Column 16 Line 43 and Column 9 Line 54 – 55).

18. As per claims 2 and 10, Tycksen teaches the claimed invention as described above (see claim 1 for both). Tycksen does not expressly teach the first software element is a driver software element.

19. Drake teaches the first software element is a driver software element (Drake: see for example, Column 16 Line 54 and Column 6 Line 13 – 16).

20. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Drake within the system of Tycksen because (a) Tycksen teaches the method of software authentication including content integrity (b) Drake discloses the software entity to be authenticated with precalculated check-data (and checksum) can be a keyboard device driver software prior to accepting the security ID-data (Drake: see for example, Column 6 Line 14, Column 16 Line 43 and Column 9 Line 54 – 55).

21. As per claim 3, Tycksen as modified teaches the claimed invention as described above (see claim 1). Tycksen as modified teaches the second software element is a content providing software application, such that the content providing software application authenticates the driver software element (Tycksen: see for example, Column 10 Line 11) & (Drake: see for example, Column 9 Line 54 – 55).

22. As per claims 5 and 22, Tycksen teaches the claimed invention as described above (see claims 4 and 21 respectively). Tycksen does not teach the third software element is instantiated in memory space allocated for drivers in said host computing system, and said first software element is a driver software element.

23. Drake teaches the first software element is a driver software element (Drake: see for example, Column 16 Line 54 and Column 6 Line 13 – 16).

24. See the same rationale of combination applies here as above in rejecting the claim 2.

25. Tycksen as modified further teaches third software element is instantiated in memory space allocated for drivers in said host computing system (Drake: see for example, Column 5 Line 65).

26. As per claim 6, Tycksen teaches the claimed invention as described above (see claim 1). Tycksen does not teach the component stored in host storage is the first software element.

27. Drake teaches the component stored in host storage is the first software element (Drake: see for example, Column 6 Line 16 – 17).

28. See the same rationale of combination applies here as above in rejecting the claim 2.

29. As per claims 7, 24 and 36, Tycksen teaches the claimed invention as described above (see claims 6, 23 and 35 respectively). Tycksen does not teach the access of the first software element stored in host storage is during runtime of the software authentication system.

30. Drake teaches the access of the first software element stored in host storage is during runtime of the software authentication system (Drake: see for example, Column 6 Line 14 – 17).

31. See the same rationale of combination applies here as above in rejecting the claim 2.

32. As per claim 8, Tycksen teaches the claimed invention as described above (see claim 1). Tycksen does not teach the component stored in host storage is a file stored on a hard drive of said host.

33. Drake teaches the component stored in host storage is a file stored on a hard drive of said host (Drake: see for example, Column 6 Line 13 – 16).

34. See the same rationale of combination applies here as above in rejecting the claim 2.

35. As per claims 16 and 29, Tycksen teaches the claimed invention as described above (see claim 1 and 19 respectively). Tycksen teaches using hash algorithm or message digest for content integrity validation.

36. Tycksen does not teach expressly said hashed result is formed from said accessed component using at least one of few, division, multiplication, variable string addition, variable string exclusive-or and double variable string exclusive-or hash function algorithms.

37. Drake teaches said hashed result is formed from said accessed component using at least one of few, division, multiplication, variable string addition, variable string exclusive-or and double variable string exclusive-or hash function algorithms (Drake: see for example, Column 16 Line 43).

38. See the same rationale of combination applies here as above in rejecting the claim 2.

39. As per claims 17 and 30, Tycksen teaches the claimed invention as described above (see claim 1 and 19 respectively). Tycksen teaches using encryption / decryption for authentication.

40. Tycksen does not teach expressly said said asymmetric encryption and decryption are performed using at least one of RSA, Diffie-Hellman, Elliptic-Curve and PGP asymmetric cryptography algorithms.

41. Drake teaches said asymmetric encryption and decryption are performed using at least one of RSA, Diffie-Hellman, Elliptic-Curve and PGP asymmetric cryptography algorithms (Drake: see for example, Column 12 Line 55 – 59).

42. See the same rationale of combination applies here as above in rejecting the claim 2.

43. As per claim 20, Tycksen teaches the claimed invention as described above (see claim 19). Tycksen does not teach expressly the first software element is a data storage device driver software element, wherein the second software element is a content providing software application, and wherein the method for authentication is a method for authentication of the data storage device driver software element by the content providing software application.

44. Drake teaches the first software element is a data storage device driver software element, wherein the second software element is a content providing software application, and wherein the method for authentication is a method for authentication of the data storage device driver software element by the content providing software application (Drake: see for example, Column 9 Line 54) & (Tycksen: see for example, Column 10 Line 11).

45. See the same rationale of combination applies here as above in rejecting the claim 2.

46. As per claim 35, Tycksen as modified teaches the claimed invention as described above (see claim 34). Tycksen as modified further teaches the accessing and hashing of said at least one portion of the component stored in host storage includes accessing and hashing at least one portion of the first software element (Tycksen: see for example, Column 10 Line 11 – 26).

47. As per claim 37, Tycksen teaches the claimed invention as described above (see claim 19). Tycksen further teaches the accessing and hashing of said at least one portion of the component stored in host storage includes the accessing and hashing of a file stored on a hard drive of said host (Tycksen: see for example, Column 6 Line 13 – 16).

48. As per claim 39, Tycksen as modified teaches the claimed invention as described above (see claim 34). Tycksen as modified further teaches comprising a storage medium and a data storage device, wherein a communications channel between the data storage device and the storage medium is authenticated with a technique including at least one of a retroreflective marker, latent illuminance marker, disk indelible utility mark (DIUM), holographic marker included on said storage medium (Tycksen: see for example, Column 1 Line 48).

49. As per claim 40, Tycksen as modified teaches the claimed invention as described above (see claim 34). Tycksen as modified teaches said hashed result is formed from said accessed component using at least one of few, division, multiplication, variable string addition, variable string exclusive-or and double variable string exclusive-or hash function algorithms (Drake: see for example, Column 16 Line 43).

50. As per claim 41, Tycksen as modified teaches the claimed invention as described above (see claim 34). Tycksen as modified said asymmetric encryption and decryption are performed using at least one of RSA, Diffie-Hellman, Elliptic-Curve and PGP asymmetric cryptography algorithms (Drake: see for example, Column 12 Line 55 – 59).

51. As per claim 39, Tycksen as modified teaches the claimed invention as described above (see claim 34). Tycksen as modified further teaches comprising a storage medium and a data storage device, wherein a communications channel between the data storage device and the storage medium is authenticated with a technique including at least one of a retroreflective marker, latent illuminance marker, disk indelible utility mark (DIUM), holographic marker included on said storage medium (Tycksen: see for example, Column 1 Line 48).

52. As per claim 42, Tycksen as modified teaches the claimed invention as described above (see claim 34). Tycksen as modified further teaches said correlation occurs when one from the following group occurs: (1) when said first and second digital signatures are identical, (2) when a portion of said first digital signature is identical to a portion of second digital signature, (3) when said first digital signature equals said second digital signature after applying a predetermined algorithm to one of said first and second digital signatures and (4) when said first digital signature maps to said second according to an interpreted off-set match (Tycksen: see for example, Column 10 Line 11 – 26).

53. As per claim 43, Tycksen as modified teaches the claimed invention as described above (see claim 34). Tycksen as modified further teaches a

computer-readable medium having computer-executable instructions for instructing a computer to perform the method recited in claim 19 (Tycksen: see for example, Column 1 Line 1 – 19).

54. As per claim 44, Tycksen as modified teaches the claimed invention as described above (see claim 34). Tycksen as modified further teaches a modulated data signal carrying computer-executable instructions for performing the method as recited in claim 19 (Tycksen: see for example, Column 1 Line 1 – 19).

55. Claims 9, 11, 13, 14, 26 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tycksen (Patent Number: US 6189097 B1), hereinafter referred to as Tycksen, in view of Sims (Patent Number: US 6550011 B1), hereinafter referred to as Sims.

56. As per claims 9. 14, 26, and 38, Tycksen teaches the claimed invention as described above (see claims 1, 19 and 34 respectively). Tycksen does not teach further comprising a data storage device, wherein the communications channel between the first software element and the data storage device is authenticated with a technique including at least handshaking algorithms with a secure memory with authentication integrated circuit included in said data storage device.

57. Sims teaches a data storage device, wherein the communications channel between the first software element and the data storage device is authenticated with a technique including at least handshaking algorithms with a secure memory

with authentication integrated circuit included in said data storage device (Sims: see for example, Column 12 Line 13 – 17 and Column 12 Line 42 – 45) & (Applicant Admitted Prior-art: Paragraph [0044] Line 18 – 20, smart card is indeed a storage device).

58. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sims within the system of Tycksen because Sims discloses the advantages using the storage device (such as dongle) for authentication purpose can enhance the security with the secure area that is not readable or directly writable by any element external to the storage device (Sims: see for example, Column 13 Line 1 – 6).

59. As per claims 11 and 13, Tycksen teaches the claimed invention as described above (see claims 10 and 12 respectively). Tycksen does not teach the second software element is firmware included in a data storage device, such that the firmware included in the data storage device authenticates the driver software element.

60. Sims teaches the second software element is firmware included in a data storage device, such that the firmware included in the data storage device authenticates the driver software element (Sims: see for example, Column 12 Line 13 – 17 and Column 12 Line 42 – 45: ROM included in most of the storage devices is a type of firmware) & (Applicant Admitted Prior-art: Paragraph [0044] Line 18 – 20, smart card is indeed a storage device and smart card also has firmware).

61. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sims within the system of Tycksen because Sims discloses the advantages using the storage device (such as dongle) for authentication purpose can enhance the security with the secure area that is not readable or directly writable by any element external to the storage device (Sims: see for example, Column 13 Line 1 – 6).

62. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tycksen (Patent Number: US 6189097 B1), hereinafter referred to as Tycksen, in view of Drake (Patent Number: 6006328), hereinafter referred to as Drake, and in view of Sims (Patent Number: US 6550011 B1), hereinafter referred to as Sims.

63. As per claim 27, Tycksen teaches the claimed invention as described above (see claim 19). Tycksen does not teach the first software element stored in the host storage is a data storage device driver software element, wherein the second software element is a data storage device, and wherein the method for authentication is a method for authentication of the storage device driver software element by the data storage device.

64. Drake teaches the first software element stored in the host storage is a data storage device driver software element Drake teaches the method is for authentication of a device driver software element stored in the memory of a host computer by an application (Drake: see for example, Column 9 Line 54: Drake

discloses the software entity to be authenticated with precalculated check-data (and checksum) can be a secured device driver software for the security ID-data, which evidently includes data storage device driver software element to store the security ID-data).

65. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Drake within the system of Tycksen because (a) Tycksen teaches the method of software authentication including content integrity (b) Drake discloses that the software entity to be authenticated with pre-calculated check-data (and checksum) can be a keyboard device driver software prior to accepting the security ID-data or a secured device driver software for the security ID-data, which evidently also includes data storage device driver software element to store the security ID-data (Drake: see for example, Column 6 Line 14, Column 16 Line 43 and Column 9 Line 54 – 55).

66. Tycksen as modified does not teach expressly the second software element is a data storage device, and wherein the method for authentication is a method for authentication of the storage device driver software element by the data storage device.

67. Sims teaches the second software element is a data storage device, and wherein the method for authentication is a method for authentication of the storage device driver software element by the data storage device (Sims: see for example, Column 12 Line 13 – 17 and Column 12 Line 42 – 45).

68. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sims within the system

of Tycksen as modified because Sims discloses the advantages using the storage device (such as dongle) for authentication purpose can enhance the security with the secure area that is not readable or directly writable by any element external to the storage device (Sims: see for example, Column 13 Line 1 – 6).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100